

COMPUTER-BASED METHOD AND APPARATUS FOR CONTROLLING, MONITORING,
RECORDING AND REPORTING TELEPHONE ACCESS

CROSS-REFERENCE TO RELATED APPLICATIONS

This application is a continuation of application Ser. No. 5 08/726,217, filed October 4, 1996, which is a continuation-in-part of application Ser. No. 08/510,327, filed August 2, 1995, which is a continuation of Ser. No. 08/229,517, filed April 19, 1994.

FIELD OF THE INVENTION

10 The present invention relates generally to the fields of telecommunications and penal institution management. More particularly, the invention relates to a computer-based method and apparatus for controlling, monitoring, recording and reporting access to outside telephone lines in a controlled, 15 institutional environment, such as a prison, military base, hospital, school, business or government organization. Specifically, this invention relates to apparatus for detecting when a called party has proceeded to bridge together one telephone call with another telephone call, through the detection 20 of dial tones, dual tone multi-frequency (DTMF) tones, special information tones (SIT), ring signals, busy signals, dial tones,

other call progress tones, or similar tone signals, without the necessity of sensing or detecting hook switch or flash signals, which may be problematic.

BACKGROUND OF THE INVENTION

5 Generally, the need to control access to outside telephone lines in an institutional environment is well recognized. In order to prevent individuals from incurring large, unaccountable telephone costs which the institution ultimately bears, one must either restrict access to outside telephone lines or institute
10 accounting controls whereby the costs of unauthorized calls can be billed to the responsible individuals.

Telephone systems in correctional environments require additional security considerations. Without appropriate controls on telephone access, inmates have been known to use the
15 telephones to harass outside parties (such as witnesses who testified against them, attorneys who prosecuted their case, employees of the courts, etc.), to perpetrate fraudulent schemes, and to participate in criminal conspiracies (such as arranging the smuggling of contraband into the prison, directing an outside
20 criminal enterprise, plotting escape attempts or credit card fraud). Therefore, it is critically important for correctional management officials to carefully plan, control, monitor and

record inmate access to outside telephone lines.

One of the most fundamental problems -- which exists both in correctional and other business-oriented institutions -- is cost control. To achieve cost control, it is critical that there be 5 individual accountability for each call that incurs a charge to the institution. Such accountability is typically achieved through use of personal identification numbers ("pins"). Before making a call from an institution telephone, an individual must enter his PIN. The telephone service provider is then able to 10 deliver to the institution an end-of-the-month telephone bill which lists, in addition to the cost of each call, the PIN or name of the individual who made the call. From this information, the institution can then collect reimbursement from individuals for the costs of certain calls.

15 While this system of end-of-the-month call accounting functions reasonably effectively in a business like environment, it does not work well in a penal institution. The reason is that inmates show little concern for phone bills they can't afford to pay. Thus, the institution is often forced to absorb the costs 20 of phone calls by its delinquent inmates. Moreover, the fact that account balances are only computed periodically -- i.e., every month, week, or even every day -- permits the inmate to accrue large, uncollectible phone bills before his access to the

phones can be terminated. Traditionally, penal institutions have addressed this problem by restricting inmates to collect calls only. This, however, still provides the inmates with relatively unlimited access to the outside world, leaving open numerous opportunities for fraudulent and criminal activity, as explained below. Therefore, in a penal environment, it is highly desirable to regulate phone access on an individual, pay-in-advance basis, and to immediately and automatically terminate an individual's phone access when his/her paid-up account reaches a zero balance.

Another problem in penal institutions is the inmates' desire to make threatening or harassing phone calls to witnesses, prosecutors, police officers, parol officers, psychologists, judges, and the relatives and family of such persons. Limiting the inmates' access to collect calls only, does not effectively address this problem, since an inmate can easily identify himself (to an operator) as someone from whom the recipient would likely accept a collect call. Rather, one should, at a minimum, provide a means that permits a potential call recipient to identify the caller as an inmate before accepting the call, whether that call is placed on a prepaid or collect basis. Conventionally, this is done by initially placing the inmate on hold and playing a pre-recorded message telling the recipient that a call has been placed from a correctional facility and that, if the recipient

wishes not to receive the call, he/she should hang up before the call is connected. This approach mitigates, but does not fully solve, the harassment problem. In particular, it is still possible for an inmate to repetitively call an outside party; 5 even if the recipient hangs up after hearing the pre-recorded message, the harassing effect of receiving repetitive calls from inside the correctional institution remains. Therefore, it would be highly desirable to provide an institutional telephone system that automatically prohibits inmates from attempting to call 10 certain outside persons. Moreover, it would also be highly desirable to provide a method and apparatus for allowing a recipient of an undesired call from an inmate to easily and automatically prohibit all future calls from that particular inmate, or from all inmates generally.

15 Still another concern in correctional institutions is the regulation of access to telephone systems. For various security and management reasons, it often desirable to restrict a given inmate's telephone access to particular phones, calling times, and to limit the length of calls, number of calls, and number of 20 calls to the same number. Also, to enhance security and discipline, it should be possible to instantaneously revoke an inmate's calling privileges, or to otherwise modify the extent of a particular inmate's calling privileges.

Correctional institutions also typically wish to monitor and/or record outgoing calls. Inmate-to-attorney calls, however, cannot legally be monitored or recorded. Moreover, certain inmates -- those who represent particular security risks -- 5 deserve live monitoring, as opposed to mere recording. Thus, it would be highly desirable to have a system which automatically initiates the appropriate monitoring and/or recording depending upon the identity of the inmate placing a call and the recipient of the call (i.e., attorney or non-attorney). Likewise, it may 10 be desirable that calls to certain numbers are to be monitored live, while others need only be recorded.

Because the message content of inmate-to-attorney calls cannot be legally recorded or monitored, such calls can serve as a conduit for the inmate's illegal telephone activity.

15 Therefore, it would be highly desirable to have a system which could passively -- that is, without in any way monitoring or recording what is actually being said -- monitor inmate-to-attorney calls to ensure that: (1) the only two people speaking on the line are the inmate and attorney, and/or (2) no DTMF 20 tones, rapid line impedance changes, off-hook conditions or voltage spikes appear on the line. Techniques for voice identification are known -- i.e. U.S. Patent Nos. 4,993,068, entitled UNFORGEABLE PERSONAL IDENTIFICATION SYSTEM and

5,150,357, entitled INTEGRATED COMMUNICATIONS SYSTEM, both incorporated herein by reference -- but have not been previously used in penal telecommunications applications.

One patent, U.S. Patent No. 4,726, 057 to Doerry et al.

5 explained many of the problems brought about by the deregulation of the telephone industry in the United States. That patent states: "Prior to a June, 1984 FCC decision, pay telephones were the exclusive province of the various Telephone Companies while others were precluded from the business of providing pay
10 telephone service. Today, however, subject to state Public Utility Commission regulations, Customer Owned Coin Telephone (COCOT) service is permitted, but a number of non-trivial technical challenges have been created including called party answer detection.

15 Coin telephones (pay phones) owned by the local Telephone Company generally utilize DC signals to signal called party answer. Such information is specially communicated between telephone central offices and then to the originating pay phone telling it when to accept the deposited coins. Such information, 20 however, is not communicated to conventional telephones and it is only with great difficulty that called party answer can be detected. Naturally, the calling party knows when a connection is completed; but a knowledge of human frailty suggests that he not

be relied upon to turn the "meter" on.

Complicating the problem of answer detection is the existence of special information messages that are provided when, for example, a telephone has been disconnected or a new telephone 5 number has been assigned; and while certain tones are indicative of a proper answer, other tones are not. Ringing, busy and reorder signals as well as background noise and feedback from the calling party herself (sidetone) make answer detection a formidable challenge."

10 The problems set forth above are exacerbated by the fact that callers, such as inmates in a prison, have the ability to work in concert with others outside of the facility. For example, an inmate may be restricted from calling a particular judge who sentenced him, however, that inmate may call his 15 spouse, who in turn may set up a conference call to the judge, thus allowing the inmate to verbally abuse the judge. Such a conference call may be prohibited by law, however, the correctional facility cannot prevent it, as the called party, in this case, the spouse, has the ability to bridge callers with 20 other outside, unrestricted telephone lines, thus giving the inmate unrestricted telephone access.

Present attempts to solve the problem of called party bridging, or so-called third party calls, have shortcomings. For

example, one attempt at resolving this problem is disclosed in U.S. Patent No. 5,319,702, to Kitchin et al. In that patent, the need to provide an apparatus for use in conjunction with so-called "local equipment/telephone." When the local equipment/telephone is in telecommunication with a remote telephone, (i.e., when a telephone call is established therebetween), the apparatus is capable of indicating whether the remote party has performed a specific act causing the generation of a hook flash-type signal which is detected by the apparatus.

5 In that patent, the detection of a hook flash-type signal is presumed to solve the problem of unauthorized calls to third parties, such as a telephone call from an inmate to the judge who sentenced him, as set forth above. The apparatus of that patent includes a band filter for passing energy having certain frequencies and an energy detector for detecting a specific electrical energy pulse having been filtered by, i.e. passed through the filter, and having a predetermined minimum magnitude. The apparatus of that patent further describes in part software (referred to as window analyzation means) which cooperates with

10 15 the energy detector to detect a specific event(s) occurring on the telephone line during a predetermined maximum time window following the detection of a specific pulse on the telephone line, i.e., when a telephone call is in progress between the

20

local party/equipment and the remote party. The detection of a specific event(s) on the line provides an indication as to whether the remote party has performed a specific act such as (1) attempting to initiate a 3-way conference call, (2) accepting a 5 call or the charges therefor, (3) terminating a call before the local equipment/party terminates the call, and (4) dialing a specific number on a remote rotary/pulse telephone. Further, the apparatus of that patent is said to be suitable for use in a computer controlled telephone wherein the energy detector detects 10 when a called party has answered a call initiated by the computer operated telephone and dialed a pulse/dial telephone or activated (flashed) the hookswitch. The energy detector is said to do this by measuring incoming electrical signal energy in a particular frequency band. Then, according to that patent, the software 15 window analyzer cooperates with the energy detector to provide efficient and reliable protection of a called party's pulse dialing of a digit (usually a "zero") to verify the called party's acceptance of a call or a collect call or the called party's attempt to activate 3-way calling by flashing the called 20 party's telephone hookswitch.

The energy detector of U.S. Patent no. 5,319,702 to Kitchin et al. is also said to include an absolute value level detector circuit that determines when an energy pulse having passed

through the band filter is above a predetermined level. If above a predetermined level, the information is transmitted by the energy detector to the apparatus' controlling computer. As previously mentioned, the apparatus further includes software, 5 i.e., the aforementioned window analyzer, for cooperating with the energy detector to detect specific event(s) occurring on the telephone line during a predetermined maximum time window following a detection of the specific pulse. In the situation where the apparatus according to that patent is said to be 10 designed or programmed to detect a remote party's attempt to initiate a 3-way conference call, the software window analyzer is said to include a timer or timer means for cooperating with the energy detector so that the timer begins running for a first predetermined period when a specific energy pulse is detected by 15 the energy detector. The software window analyzer also includes sound detection means for detecting sound on a telephone line and for cooperating with the timer so that the sound detection means is activated at the end of the first predetermined period for a second predetermined maximum time period. If sound is not 20 detected during the second predetermined time period, such indicates that the remote party has attempted to initiate a 3-way conference call.

Kitchin discloses a type of energy detector that can also

incorporate a ringback detector -- not to activate third party
call blocking, but merely for activating the energy detector when
the ringback signal is detected. Thus, the ringback detector is
used to set the energy detector, so that the energy detector can
5 purportedly carry out the purpose of that patent, and so that the
energy detector can be utilized. Indeed, Kitchin states that
"[t]hose skilled in the art will appreciate that called party
answer is indicated when the first specific energy pulse is
detected after the apparatus has detected the called party's
10 ringback signal." Thus, the ringback signal is used to
initialize the Kitchin system -- not to solve the problem at
hand. In that sense, Kitchin teaches away from relying upon the
use of ringback detection as a means to block third party calls.

The Kitchin patent discloses "being useful for detecting
15 certain specific events, i.e., call answer, an attempt to
initiate a 3-way conference call, call acceptance, call
termination, and determining the specific number dialed number on
a rotary/pulse telephone. Any event which causes the generation
of the hook flash-type signal such as a call waiting signal can
20 purportedly be detected. Importantly, Kitchin says that it can
detect "any event which causes the generation of the hook flash-
type signal". This is important because that is the entire focus
of the Kitchin patent -- to detect hook flashes, or the energy

pulses associated therewith. This approach is problematic, as it relies on the detection of a pulse -- not the detection of certain tones. While the Kitchin patent may appear to be an elegant solution to the problem of blocking third party calls, 5 it is needlessly complex, and if anything, complicates the process of detecting the attempted establishment of third party calls. The prior art does not teach the simple, direct method of sensing third party call patterns by merely monitoring the occurrence of tones that called parties traditionally generate in 10 their efforts to bridge callers with third parties. In essence, many called parties allow the caller to be on the line while they dial the third party -- that is an opportunity to sense DTMF tones. Then, many called parties may dial the wrong number of the third party, and a SIT tone will indicate that number may 15 have been disconnected, subject to an area code change, or the like -- all while the caller is on the line. That is another opportunity for sensing tones to prevent third party calls. Also, called parties may use a credit card to call third parties -- also while the caller is on the line. Call progress tones may be 20 generated during such credit card calls -- thus, yet another opportunity to sense tones to prevent third party calls. Also, if at any time during the call, a ring or busy signal is heard on the caller's telephone, still another opportunity is present for

sensing tones to prevent third party calls. And finally, if at any time during the call while the inmate is on the line, a dial tone occurs (as when a called party may go off-hook to place the call to the third party), yet another opportunity exists for 5 sensing tones to prevent third party calls.

SUMMARY OF THE INVENTION

In light of the above, one object of the invention is a method of managing telephone activity in an institutional 10 environment to achieve improved security and reduced cost.

Another object of the invention is a system adapted to perform such improved institutional telephone management.

Yet another object of the invention is a method and apparatus for passively monitoring a telephone connection to 15 detect security breaches.

A still further object of the invention is an institutional telephone management system wherein the parameters that control the operation of the system as well as the records of system activity are stored in a central database, thereby permitting 20 simple customization of system operation, generation of reports and monitoring of status.

In accordance with one aspect of the invention, a method of managing telephone activity in an institution includes the steps

of: (1) identifying an institutional caller (the "calling party") who wishes to place an outside call to an outside recipient (the "called party"); (2) blocking the institutional caller and -- while the institutional caller's line (earpiece and/or 5 mouthpiece) remains blocked -- (a) calling said outside recipient (called party), (b) providing the identity of said institutional caller to said outside recipient and [©] receiving a control code from said outside recipient; (3) determining, in response to said control code, whether to connect the institutional caller to the 10 outside recipient, and optionally, whether to indicate any of a plurality of messages to the calling party, e.g., an inmate, and (4) terminating or otherwise tracking or accounting for calls to third parties whereby attempts are made by the called party to bridge or conference the calling party (the caller or inmate) 15 with any third party.

In accordance with another aspect of the invention, an apparatus for managing telephone activity in an institution includes: a plurality of institutional telephones located within the institution; a trunk management unit (TMU) for selectively connecting the institutional telephones to one or more outside telephone lines, wherein the TMU includes means for decoding DTMF tones generated by the institutional telephones or received from the outside telephone lines; and a computer control unit (CCU),

coupled to the TMU, for controlling the connection of the institutional telephones to the outside telephone lines based upon DTMF tone(s) received from the outside telephone lines. A database associated with the CCU contains information regarding 5 the calling privileges of each person within the institution. In a preferred embodiment, the TMU -- prior to connecting the call -- plays an announcement to the called party identifying the institution and caller, along with the options available to the called party. In response, the called party may enter the 10 announced DTMF tone sequence (preferably GOTU), which modifies a record in the database, thereby prohibiting the caller (and/or other similarly situated prospective callers) from calling the called party in the future.

Other features of the TMU provide security and monitoring 15 functions. The invention provides three levels of monitoring, any or all of which may be active for any given call. The first level is "live" call (voice) monitoring, where the prison officials actively listen to a live call. The second level is call recording. The TMU can be programmed to enable associated 20 recording equipment to record telephone calls. The third level is "passive" line monitoring, where the TMU detects, for example, DTMF tones, off-hook conditions, voltage spikes and/or sudden line impedance changes, in order to thwart attempts at

unauthorized three-way calling, call conferencing, call transferring, call forwarding or re-dialing via various alternate common carriers, many of whom now offer "1-800" or local telephone number (e.g., "950") access numbers. Also, care is 5 taken to avoid disrupting calls that do not represent security breaches, by preventing false triggering of the above "passive" line monitoring features. For example, with respect to DTMF tone blocking, the TMU will look for any additional digits entered by an institutional caller, such as an inmate, to prevent the inmate 10 from redialing to other telephone numbers that may not be authorized. However, to prevent "talkoff", whereby the normal telephone conversation can falsely trigger a disconnect signal (because the TMU may interpret the conversation as DTMF dialing), the TMU can be set to look at the number of digits dialed within 15 a specified time period (e.g., six (6) digits within a fifteen (15) second time period, or any variation of the two parameters) and thereby, determine whether the audio information is indicative of unauthorized DTMF redialing or just a normal speech or voice pattern.

20 In accordance with the preferred embodiment of the invention, all calls are passively monitored and all calls that can be legally recorded -- i.e., all but inmate-to-attorney calls -- are recorded. At any time, prison officials can selectively

invoke live monitoring to listen in on any call in progress, except an inmate-to-attorney call. System alarms, which trigger any time a particular inmate places a call or calls a certain person, allow officials to determine when live call monitoring is appropriate. Likewise, the telephone system of the present invention can be programmed to default in any manner. For example, the system can be set to place only those telephone calls that are among a pre-approved list of telephone numbers. Conversely, the system can be set to place all telephone calls except those that are among a list of restricted telephone numbers. Optionally, the telephone system of the present invention can include speed-dialing, whereby upon entering a PIN, for example, an inmate can enter "11" followed by the "#" key. In that case, the prison administrator may have established that "11" is the speed-dialing sequence for that inmate's mother. Of course, the system could be configured so that the inmates themselves can program the telephone system with speed-dialing digits, however, a principal objective of speed-dialing is to save time at the telephone, thus making the telephones available to the largest number of inmates in the shortest possible time period.

In addition, the invention may include biometric voice verification features. The TMU, for example, may digitize a

sample of the caller's voice. The CCU then compares the digitized sample with a stored voice print, to verify the identity of the caller. Such biometric monitoring may also be used in a passive call monitoring mode, wherein periodic samples 5 of the caller's voice are provided to the CCU -- and checked against a list of authorized voice prints -- to ensure that no unauthorized callers are participating in a call, and to ensure that inmates are not sharing or selling relatively liberal calling privileges associated with a particular PIN or inmate 10 account to other inmates that are subject to more limited calling privileges. The use of biometric voice verification (or "voice prints") can prevent PIN abuse in general. For example, if a particular inmate with restricted calling privileges, or no available funds, attempted to force (e.g., by threatening 15 physical attack) another inmate with relatively non-restricted calling privileges (or available funds) to turn over his PIN, biometric voice verification would obviate this problem, as the voice would be used to validate entry into any inmate account.

The principal feature of the present invention is the 20 implementation of a way to detect inmate or other regulated caller telephone calls to called parties, whereby said called parties act to bridge the inmate or regulated caller to some third party. Whereas regulated callers, by definition herein,

are only permitted to communicate with certain called parties, the authority in charge of the caller or inmate's calls are afforded the ability of preventing called parties from bridging telephone calls from inmates or other regulated parties to 5 unauthorized or unknown third parties. Said authority has, at its option, the ability to prevent, terminate and/or track or monitor any of said attempts.

Broadly, the present invention takes the form of an apparatus and method for detecting and identifying disparate 10 preselected signal sequences of spaced tone bursts. Such spaced tone bursts or tone signals may be originated by the called party in a called party's effort toward bridging the caller or inmate with a third party. Such tones are the tones often generated during such bridging attempts, such as the ringing of the third 15 party's telephone, a busy signal during the attempted calling of a third party by the called party, a dial tone as the called party is dialing the number of the third party, SIT tones generated when the called party attempts a telephone call to a third party whose number has been, for example, disconnected, 20 other call progress tones, such as those associated with telephone credit card usage, other DTMF tones, for example, those used by the third party to call the third party in the first place, and any other tones, thus obviating the need for any

detection of hook flashes or other clicks and/or pops on the telephone line, that may unreliable be associated with attempts by called parties to place telephone calls to third parties.

In some further specific aspects of the invention, logic 5 circuitry comprises gates and registers. The latter is used to store durations of tone bursts and spaces which the gates compare for consistencies with a preselected signal sequence. Further gates are utilized to detect one of a plurality of preselected error conditions. Occurrence of an error condition is used to 10 override indication of a valid signal sequence and to identify possible malfunctions in apparatus used to generate the preselected signal sequences. The storage of certain tones may be desired, for example, with ring or busy signals. As those tones are often associated with specific cadences (ring 2/3 on, 15 1/3 off, and busy 50% on, 50% off), the sensing of cadence in addition to tone frequency can improve system reliability. The detection of tones can be accomplished by certain integrated circuits, such as the Teltone brand series of chips, designed to 20 detect and digitally decode DTMF and/or SIT tones. Typically, DTMF tones are the 12 conventional Touch Tones (1-9, 0, # and *), and SIT tones are generated by the local central office equipment when a call does not go through, for example, if a number is blocked from a particular telephone number, a number is no longer

in use, a number has been disconnected, an area code has been changed, etc. With the present invention, such tones (DTMF or SIT), or other tones (dial, ringing, busy or call progress tones) are used to signal an inmate or other regulated telephone system 5 that a called party (a party called by, e.g., an inmate) is attempting to bridge that telephone call together with some unknown and/or unauthorized third party. Upon the detection of such a tone (call progress tone or other tone), the present invention may either terminate the call between the inmate and 10 the called party, or may evaluate what third party was called, to attempt to validate such a third party call.

Also, with the present invention, the third party call attempt may be stored, for present or future review by an institutional authority, and patterns may be monitored, so that 15 prison officials may consider curtailing future inmate calls to particular called parties. Thus, third party call attempts can be tracked, both on a per inmate and on a per called party basis. Thus, if inmates A through G all know to call a certain called party X so that called party X can bridge them to their 20 respective unauthorized third parties, then, the prison officials will know that future calls to party X are to be blocked, regardless of who is initiating such a call, because called party X is suspected of being an individual who facilitates

unauthorized third parties. Importantly, certain called parties may even attempt to bridge a call from one inmate to another call from another inmate. In that instance, keeping track of such attempts, and terminating such calls, is particularly important, 5 as inmates within the same institution may be conspiring to do crime, such as breaking out of prison.

The present invention relies on some of the same circuitry used by certain customer owned coin operated telephones (COCOTS) and other facility based PBX equipment. Some such pay telephone 10 stations are provided with apparatus for detecting when a called party has answered a call (initiated at the coin telephone station) by tracking call progress tones, and sensing tone cadence. The apparatus of the present invention may also include circuitry for inhibiting the indication of called party 15 answer when a sequence of three predetermined (such as SIT) tones are received; such tones generally precede an intercept message such as one that announces that a telephone number has been changed or disconnected. The apparatus further includes circuitry for inhibiting the indication of called party answer when call 20 progress tones are detected. Finally, the present invention can sense DTMF tones themselves, often used in the completion of calls by Touch Tone telephones.

The present invention thus obviates the need to rely on

sensing clicks or pops associated with attempts by called parties to bridge calls via conference call circuitry or call waiting.

Such reliance is disadvantageous. First, depending upon the local exchange carrier switch, call waiting and call

5 conferencing, as provided by the telephone companies, may not even generate any click or pop (or other suitable pulse that could activate the Kitchin circuitry). Also, the circuitry of

Kitchin is susceptible to false triggering, as it senses impulses that can occur randomly. To the contrary, applicant contends

10 that the invention set forth herein is simpler and more accurate, certainly insofar as false triggering is concerned. Applicant contends that the sensing of tones exclusively as a means to restrict third party calls will lead to far less false triggering as compared to the Kitchin proposal. As applicant's invention is

15 not directed to sensing third party call attempts that do not involve tones, applicant senses only tones -- not impulses associated with hook flashes, as Kitchin requires. To the contrary, applicant contends that the present invention obviates the need for that by sensing other criteria that may be

20 indicative of an attempt by a called party to bridge one telephone caller with another.

BRIEF DESCRIPTION OF THE DRAWINGS

The detailed description below describes the preferred embodiments of the invention and is intended to be read in conjunction with the set of drawings, in which:

5 Fig. 1 is a block diagram showing the major components of a preferred apparatus, including a plurality of institutional telephones, a computer control unit (CCU) and a trunk management unit (TMU);

10 Fig. 2 is a block diagram showing the software and firmware architecture of the TMU/CCU apparatus;

Fig. 3 is an exemplary screen showing an institutional user's calling privileges and activity;

Fig. 4 is a block diagram of a TMU;

15 Fig. 5 is a block diagram of a TMU and CCU/CPU configured which permits third party calls to be detected; and

Fig. 6 is a flow diagram depicting the operation of applicant's third party call detection system.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

20 The preferred embodiment(s) will be described with reference to prison based call management. This, however, should not be viewed as limiting, since the invention is also applicable in

other institutional settings such as military bases, schools, mental institutions and business organizations.

Referring now to Fig. 1, a call management system manages calls from a plurality of inmate telephones 1. A TMU 2 controls the connection of individual inmate telephones (for example 1a) to outside telephone lines 8, and electronically monitors connected calls. A TMU 2 can optionally contain (and/or be connected to external) voice messaging or voice synthesis equipment, to facilitate features such as over-the-phone voice prompting, voice mail, or any voice activated, responsive or interactive telephone feature. For example, an inmate could enter his/her PIN into a telephone 1 keypad, and then, access his/her account. In turn, voice equipment associated with or contained within the TMU could inform the inmate of the exact balance available in his/her account for future telephone calls. Additionally, the inmate could ascertain how much any prior telephone call has cost, and further, could dial an intended telephone call, and ascertain how much that call will cost for the first time period (e.g., the first minute), or, find out how many minutes the inmate can be connected to that telephone number, given the cost of that call and the amount remaining in the inmate's account, all prior to actually completing the call and becoming obligated to pay for it. Obviously, for debit-based

systems, inmate calls will not be placed in the event that sufficient funds are not available. Further, if during a call connection, inmate funds become nearly exhausted, a warning tone could inform the inmate of that condition, so that the inmate can 5 terminate the conversation, and take appropriate steps to replenish his/her account. Such warning tones could be made possible by a real time call cost monitoring system, that compares inmate call costs and inmate account balances while each call is in progress.

10 A serial interface card 4 digitally interfaces TMU 2 to: a CCU 3, one or more administrative terminals 5a-b and, via data modems 6a-b, and to a remote terminal 7. Of course, remote terminals 7, administrative terminals 5 and CCUs 3 can be connected via so-called dedicated data/telephone line services, 15 obviating the need for actual modems 6. Alternatively, TMUs 2 may share a common local area network. Such an alternative structure can accommodate data transfers, digitized voice signals, data packet transmissions, call processing data, and the like. In such an alternative embodiment, the local area network 20 may even facilitate packet communications between individual TMUs or the TMUs and their respective hosts.

TMU 2 communicates bi-directionally with CCU 3. In one direction, CCU 3 directs TMU 2 to connect, record, passively

monitor and terminate calls, and to download and/or play prerecorded messages to an inmate or outside call recipient. In the other direction, TMU 2 monitors the real-time status -- i.e. off-hook, DTMF tones, voltage spikes and rapid impedance changes

5 -- of institutional and outside telephone lines. In addition,

TMU 2 can provide digitized voice samples to CCU 3 in order to record messages (such as the inmate's name) and to support biometric voice verification or monitoring functions.

Optionally, TMU 2 (or other comparable apparatus) could be

10 configured to provide digitized voice samples to, for example,

CCU 3, for each call made, whereby such samples are sufficient in length to provide verification that the inmate indeed participated in a conversation with a particular called party on a particular date and at a particular time. Because prison

15 administrators may not wish to charge inmates (or in the case of collect calls, called parties) for certain calls (for example, calls the administrator deems incomplete), it is critical that administrators have the ability to verify actual telephone

communications. Incomplete telephone calls may include, for

20 example, busy signals, calls that do not "go through", calls that are not answered (as distinct from calls that reach answering machines, which may be deemed complete), etc. Thus, if an inmate or a called party subsequently claims that a particular telephone

communication never occurred (e.g., a busy signal was reached, the called party never answered, or no voices were spoken at all), the prison administrator can retrieve the voice verification record to evaluate whether, e.g., a credit is due, 5 telephone system repair is required, or whether claims that certain calls were incomplete are false.

Referring now to Fig. 2, CCU 3 is preferably a "486" personal computer or larger "super-mini" type computer configured to operate under a suitable operating system, such as UNIX™ 10 System V. Of course, any number of operating systems will be suitable for the purpose of the present invention. In addition to the operating system, a database management system (DBMS), such as ORACLE™, which includes a structured query language (SQL) interface, is used to store system configuration and status 15 information. A SQL forms generator provides access to the stored configuration and status information. A SQL menu program allows users to easily navigate the database system. A SQL report writer is used to generate reports of calling activity or other system usage.

20 TMU firmware controls the operation of TMU 2. TMU interface software in CCU 3 is configured to manage communication between TMU 2 and CCU 3. ORACLE interface software provides a simple, menu based interface to field users such as correctional officers

and management officials. Real-time control software manages the real-time activity of the system and responds to communications from TMU 2 and user inputs from CCU 3 or terminals 5a-b and 7.

From an administrator/user perspective, the CCU software
5 supports the following general functions:

- (1) establishment and configuration of individual inmate data and monetary accounts;
- (2) checking of inmate debit (i.e. paid-in-advance) accounts;
- (3) setting of global (i.e. institution wide) and individual restrictions on telephone access;
- (4) real-time monitoring of inmate telephone calls and alerts (based on call content, security breaches, etc.), along with the ability to cut off inmate calls individually or globally;
- (5) storing and reporting of detailed inmate call details and account information; and
- (6) storing and reporting of telephone usage data.

Referring now to Fig. 3, an exemplary form 30 provides easy
20 access to various information regarding an inmate's debit account, calling privileges and calling activity. The Fig. 3 form includes a title segment 31, which displays the current date, title of the form and form code. Below the title segment

is a header segment 32, which typically displays such information as the inmate's name, registration number, preferred language selection, prisoner account code ("PAC", or PIN), certain calling privilege information and account balance. Below the header are

5 a plurality of data blocks 33, which show the inmate's transactions (both accounting transactions and phone calls) as well as his/her calling privileges and restrictions -- i.e., numbers the inmate is allowed to call, the inmate's attorney's number, numbers the inmate is prohibited from calling, and

10 numbers which should trigger an alert on the system terminals when a call is attempted. The system allows the user to scroll through the data blocks in order to bring any particular transaction or restriction into view. A help line 34 lists the commands available to the user. A bottom positioned status line

15 35 completes the form. Form 30 may be expanded as desired to facilitate keeping track of which inmates have attempted to call called parties, who in turn make an effort to conference in a third party. Where the called party has the inmate on the line while the called party dials the third party, the TMU may sense

20 the telephone number of the third party, and record that information as well in form 30. Thus, form 30 may contain a listing of the called numbers (as in segment 33), and may also contain the numbers that the called parties attempt to bridge

together with the inmate. Also, other forms like form 30 may be generated on a per third party basis. In that manner, if multiple inmates tend to call the same called party, and that called party tends to bridge inmates to unauthorized third parties, including even to other inmates, the prison officials can read such a report, on a per third party and/or even called party basis, to evaluate whether to restrict inmate calling privileges, and to evaluate whether to restrict calls globally to one particular called party.

Referring now to Fig. 4, a block diagram of one channel of a multichannel TMU 2 is shown. Generally, TMU 2 includes circuitry to selectively connect inmate phones with outside lines, to selectively monitor and record the connection, and to generate appropriate voice instructions or prompts to the inmate and/or the outside call recipient.

As depicted in Fig. 4, a channel of TMU 2 connects to an inmate telephone 1 at a station input line 40. A record blocking circuit 41 connects station input line 40 to recording equipment (not depicted) via line 41a (which line can also be used for "live" call monitoring). CCU 3 automatically controls an attorney relay 41b and, in the case of an inmate-to-attorney call, switches line 41a to a tone generator 41c, thereby blocking improper attempts to record or monitor inmate-to-attorney calls.

A split relay 42 switches the inmate telephone between a local line 42a and an outside line 42b. Initially (i.e. before the inmate initiates a call), split relay 42 connects station input line 40 (via local line 42a) to a monitor circuit 43, which 5 monitors the inmate's telephone. Monitor circuit 43 supplies a battery feed to the inmate's telephone, and performs pulse digit recognition and current detection as well. A dial tone generator 43a (which is preferably common to all channels of the TMU) supplies a dial tone to the inmate's phone. A relay 44a switches 10 a DTMF receiver 44 to decode tones on the local line 42a or the outside line 42b. A voice-out-station line 45a supplies voice messages to the inmate's telephone. CCU 3 controls the decoder portion of an integrated coder/decoder (CODEC) circuit to generate the messages fed to line 45a. (The decoder portion of a 15 second CODEC also drives a voice out central office line 45c to play messages to outside line 42b.) A central office voice input line 47b connects to the coder portion of the CODEC circuit to support message recording, voice monitoring and/or verification functions. Optionally, voice-in-station 42c is used to record 20 the name of an inmate. Also optional, answer board line 47g is used to detect called party answer conditions, by detecting the presence or loss of call progress tones (e.g., ringing, busy, special-information-tones (SITs), etc.).

A hold circuit 46 is used to interact with the outside caller during the call qualification process, during which the station input line 40 is switched to local line 42a. A hold relay 46d selectively connects hold circuit 46 to outside line 42b. A DTMF generator 46c (preferably common to all channels of the TMU) is controlled by CCU 3 to, for example, place an outside call to a requested number. Hold circuit 46 interfaces with DTMF receiver 44 to detect tones generated by the outside caller during the call qualification process. The hold circuit 46 (with its associated relay 46d) can also pass audio information directly to the monitor circuit 43 as desired via audio feed through line 46b. The hold circuit 46 can also be used for dial-pulse dialing to the central office. Line current detector 47a (preferably implemented using an opto-isolator), ring detector 15 47e, and tip/ground detector 47d monitor the status of outside line 42b. Ground start relay 47f connects a ground start circuit to the ring wire of outside lines 48a and 48b, to start "ground-start" type lines. A line relay 48 switches outside line 42b between a central office main line 48a and a central office auxiliary line 48b. Also shown are voice out (45c) and voice in (47b) ports, and a ground start (47c).

In addition to the channel circuitry described above, TMU 2 is controlled by a microprocessor 49a, which interfaces with a

watchdog timer 49b and with a memory 49c, channel I/O 49d, miscellaneous I/O 49e and dual serial ports 49f via data, or so-called "glue" logic 49g. TMU 2 also includes a jack tester circuit 49h and connectors 49i and 49j to answer and voice boards, respectively. The voice board contains a plurality of integrated CODECs (preferably two per TMU channel) as well as circuitry needed to permit CCU control of the CODECs, including I/O circuitry and voice data buffers.

Referring now to Fig. 5, a block diagram of a TMU 2 and CCU/CPU 3 are configured to permit third party calls to be detected. The TMU 2 includes or is interfaced to (as shown in Fig. 4, via connectors 49i and 49j) an operator board 400 and an answer supervision board 420. The answer supervision board 420 detects specific tone frequencies, and sends messages to the operator board 400. The answer supervision board 420 is capable of detecting the presence of any tones of interest, particularly with respect to the present invention, tones that may be indicative of attempts by a called party to place calls to third parties, so that the called party can bridge the caller or inmate with a third party, including unauthorized third parties. Of course, some institutions will prohibit all calls to all third parties.

Specifically, answer supervision board 420 will detect

certain frequencies of interest. First of all, the answer supervision board should be able to detect dial tones, which are typically tones consisting of components at 350 & 440 Hz. Also, answer supervision board 420 should be able to detect busy signals (a combination of 480 & 620 Hz), ring signals (440 & 480 Hz), and the like. Thus, at least four frequencies are of interest (350, 440, 480 and 620 Hz). In addition, the answer supervision board 420 may contain or may be supplemented by hardware such as the Teltone brand chip suitable for sensing and 10 decoding DTMF tones, SIT tones, other call progress tones, such as credit card validation tones, and the like. In that manner, answer supervision board 420 or other similar hardware and/or software can be established to detect tones indicative of attempts to complete third party or three-way telephone calls.

15 The operator board 400 communicates with the answer supervision board 420. The operator board determines pulse width and the edges on the tones. Also, as the operator board interfaces directly with CPU/CCU 3, operator board 400 must ignore tones which occur prior to the called party answering the 20 telephone. If not, it is possible that the ringing of the called party (which is permissible) may disconnect the inmate. Thus, the monitoring of third party calls should preferably commence only after the called party answers the telephone.

Finally, CPU/CCU 3 is responsible for interpreting detected tones and taking the appropriate action. For example, CCU# may disconnect a call to a caller upon sensing a dial tone. It may also record the number the called party attempted to connect the 5 inmate to, and it may record the number of the called party (of course). It may keep track of call history on a per inmate, per caller, per called party basis, and the like. The CCU 3 may compare the third party calls to a list of authorized calls. For example, if one particular inmate calls his attorney (a permitted 10 call), and that attorney has received permission to set up a conference call with that inmate's physician, then, CCU 3 can be programmed to permit that caller (the attorney, based on the attorney's telephone number), to conference in only that physician (based on that physician's telephone number). In that 15 manner, some third party calls could be permitted, while other are not. Also, with such a mechanism, it is contemplated that at one level, all third party calls are prohibited. Consequently, by hardware and/or software, all third party calls will be blocked, by applicant's invention or other methods of 20 accomplishing the same result. Then, by applicant's invention, the called party will be responsible for keeping the inmate on the line (via an audio communication pathway), so that the inmate can "hear" the DTMF tones that the called party is dialing, to

reach the third party. In that manner, the telephone number of the third party can be compared within the CCU against a list of approved third party number for that inmate, and the CCU 3 may permit such a third party call, by overriding the blanket

5 prohibition of all third party calls, for that one instance. In that manner, some third party calls may be permitted, and others not. Of course, the prison authorities may specify any level of prohibition or permissive third party calling, and the CCU 3 can be programmed to handle any level, and keep track of any level.

10 The CCU 3 can also handle other functions, such as taking appropriate measures in response to certain tones. Also, the tones may be monitored for their frequencies, pulse widths and even period, duration, cadences, etc. For example, busy signals are often a 50% on, 50% off cadence, while ring signals are usually 33 and a third percent on, and 66 and two-thirds percent off. Thus, CCU 3 can be used to detect signal characteristics, such as cadence, to ensure that the correct tone signal has been interpreted.

15 Fig. 6 is a flow diagram depicting the operation of one example of applicant's third party call detection system. The answer supervision firmware 600 senses whether a tone has been detected (602). If so, the duration of the tone is sensed, and if over 120 ms (604), and under 5000ms (606), then a message

(608) is sent to the operator firmware (620). It will be
recognized that the operator firmware (620) corresponds to the
operator board (400), while the answer supervision firmware (600)
corresponds to the answer supervision board (420). If the
5 operator firmware (620) receives a message (622) from the answer
supervision firmware (600), and if the called party has answered
his or her phone (624), and if the call lasts beyond 5 seconds
(626), a message (628) is sent to the 3-way call monitor program
(640), which is implemented by hardware, such as CCU 3 and
10 software. Program (640) senses messages (642) from the operator
firmware (620), and if a message was received, certain decisions
and actions are taken. First, two tones must be detected (644)
by the answer supervision firmware (600). This is so because
dial tones, ring tones, busy tones, SIT tones, DTMF tones, call
15 progress tones, etc., are all two-frequency tones, and hence,
step (644) filters out those tones that are mono-tones. Also,
particularly with respect to ring signals and busy signals, the
cadence can be sensed (646), and if a match is found, the call
can be cut-off (648) and ended (650), and the TMU 2 can be
20 released (652).

Naturally, many variations of this apparatus are possible,
so that any particular tone sequence can effect any desired
operation. Also, records of call history, attempts to bridge

calls, and any other statistics, can be kept as well, as CCU 3 can be a computer with any desired database.

Generally, the method of connecting an inmate call was discussed in the parent applications hereto, Ser. No. 08/510,327, 5 filed August 2, 1995, which is a continuation of Ser. No. 08/229,517, filed April 19, 1994, herein incorporated by reference.

TMU 2 continuously monitors the inmate telephones 1. To place a call, an inmate picks up a phone and enters two numbers 10 (in any order established by the facility): (1) his/her personal identification number (PIN); and (2) the number to be called. TMU 2 forwards both numbers to CCU 3, which, in turn, queries the inmate's account to check whether:

- (1) there are sufficient funds in the inmate's debit 15 account to make the call (unless the call is a collect call);
- (2) the particular inmate is allowed to: (a) use the particular telephone extension; (b) place calls at the given time-of-day; or [©] has exceeded a maximum 20 number of calls or calling minutes within a given period of time; and
- (3) based upon the number to be called, whether the number is approved or prohibited, whether the

number to be called corresponds to the inmate's attorney (in which case, the conversation will not be recorded or "live" monitored), and whether there are any time-of-day or call frequency or other restrictions on the number to be called.

5

If the call is rejected on the basis of (1)-(3) above, CCU 3 directs TMU 2 to play a message to the inmate (in the inmate's preferred language, determined by his/her PIN and established when the prisoner first enters the facility) explaining the reason that the call has been rejected. Assuming that the requested call has passed these initial screening tests, CCU 2 directs TMU 2 to call the destination party. Until completion of these steps, the inmate's earpiece and mouthpiece remain blocked (with respect to the called party), thereby eliminating the inmate's opportunity to interject offensive or harassing remarks.

10

15 Subsequently, the destination or called party receives the call and hears a prerecorded message which identifies the institution, caller and gives instructions as to how the called party may elect to receive the call and how the party may block future calls, if desired. The message may also state that third party calls are prohibited for this inmate (if that inmate is restricted from third party calls), or the message may indicate that third party calls are prohibited for all inmates at that

20

institution. Also, the message could ask for an authorization code, which the caller can enter, to override the third party blocking mechanism. In that manner, the attorney of the inmate, who may have gained a court order permitting third party calling, 5 can enter the password to establish a third party call -- either on his own, or by way of prison facility trunk lines. Also, the called party can be warned that the prison is aware that the called party previously completed a third party call, and if that called party does it again, they will be pursued by government 10 officials. Also, automatic number identification (ANI) can be used to locate the called party that has completed such third party calls, so that the called party can be pursued, and forced to stop the offensive activity.

Typically, in many inmate systems, the pronunciation of 15 inmate's name is stored once in the database and retrieved each time the message is generated. This eliminates the risk of an inmate interjecting a short message in place of his/her name. The pronunciation of an inmate's name may be synthesized from well-known commercially available electronic phoneme sets, or may 20 be reproduced from a voice data file created by the actual inmate or administrator. For example, when an inmate first enters a corrections facility, he/she may be instructed to recite his/her name into a voice recorder via a microphone. Then, that voice

can be stored permanently into a file associate with that inmate's calling account and/or PIN, and can be automatically replayed as desired.

In most cases, the called party is allowed a specified time 5 to determine whether to accept the call, hang up or press a code, such as GOTU, to invoke the invention's prospective call screening feature. During this period, TMU 2 monitors the line and transmits any received DTMF tones to CCU 3. As provided herein, that monitoring does not interfere with the detection of 10 third party calls.

The detection of tones is well-known in the art. In U.S. Patent No. 4,726,057 to Doerry et al., the detection of tones, such as SIT tones, is disclosed, and that patent is hereby incorporated by reference. In that patent, several drawings 15 illustrate how tone detecting circuitry may be formulated.

While the invention has been described with reference to one or more preferred embodiments, such embodiments are merely exemplary and are not intended to be limiting or represent an exhaustive enumeration of all aspects of the invention. The 20 scope of the invention, therefore, shall be defined solely by the following claims.